

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

MEATS BY LINZ, INC.,	§	
	§	
Plaintiff,	§	
	§	Civil Action No. 3:10-CV-1511-D
VS.	§	
	§	
STEVE DEAR d/b/a THE SUPREME	§	
FOODSERVICES GROUP,	§	
	§	
Defendant.	§	

MEMORANDUM OPINION
AND ORDER

In this action arising from the alleged misuse of a former employer's confidential business information, defendant's motion to dismiss under Fed. R. Civ. P. 12(b)(6) presents the question whether plaintiff has stated claims for violations of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, breach of contract, or conversion on which relief can be granted. For the reasons that follow, the court concludes that plaintiff has stated plausible CFAA and breach of contract claims on which relief can be granted, but has not pleaded a plausible conversion claim. The court therefore grants in part and denies in part the Rule 12(b)(6) motion to dismiss but also grants plaintiff leave to replead.

I

Plaintiff Meats by Linz, Inc. ("MBL") supplies meats to restaurants, hotels, and other food vendors.¹ MBL hired defendant

¹In deciding Dear's Rule 12(b)(6) motion to dismiss, the court construes MBL's complaint in the light most favorable to it, accepts as true all well-pleaded factual allegations, and draws all

Steve Dear ("Dear") to work in national sales and later selected him as General Manager of its Dallas sales facility. As General Manager, Dear handled daily operations of the facilities and had access to confidential business information, such as customer contact information, pricing, cost of goods sold, and sales histories.

MBL alleges that this customer information—which is maintained in password-protected computer hard drives and not shared with competitors—provides MBL a competitive advantage because MBL possesses unique knowledge of customer buying habits and business practices that are not readily known to its competitors. MBL protects this information by providing password access only to those employees whose duties require use of this information, and paper copies are only circulated internally to employees who need the information as a part of their duties.

During his tenure at MBL, Dear entered into a restrictive covenant agreement that precludes him from disclosing this confidential business information to others without MBL's express consent; becoming employed in a position involving buying or selling of meats that is in direct competition with MBL in Dallas or Tarrant County, Texas; soliciting any customer or former customer to purchase the same type of products that MBL sells; or

reasonable inferences in its favor. See, e.g., *Lovick v. Ritemoney Ltd.*, 378 F.3d 433, 437 (5th Cir. 2004).

engaging in activities that disparage or undermine MBL products, reputation, or business opportunities. In exchange for Dear's commitment, MBL disclosed to Dear its confidential business information and provided him employment.

MBL alleges that, on Sunday, February 28, 2010, at about 9:15 p.m., Dear accessed an MBL company computer from a remote computer to obtain a confidential MBL Gross Profit Report listing each of MBL's Dallas- and Fort Worth-area customers, together with the pricing, cost of goods sold, and profit margin for each customer. About two hours later, at 11:24 p.m., Dear resigned from MBL in an email, even though he had never before expressed such intentions. Dear then began soliciting MBL's customers and distributed business cards that identified him as associated with Supreme Food Service Group ("SFSG"). SFSG appears to be based at the same address occupied by Crystal Creek Cattle Co., Inc., one of MBL's direct competitors. One of MBL's customers, Culpeppers Cattle Co., began buying meat products from SFSG fewer than three weeks after Dear resigned. Dear was also observed calling on Tillman's Roadhouse, a Fort Worth restaurant and MBL's customer, on April 28, 2010, after he resigned as an MBL employee. Based on this information, MBL alleges that Dear used the contents of the Gross Profit Report to solicit and sell meat products to several of the accounts listed in the report.

MBL sues Dear for downloading confidential information without

authorization for use in his business, in violation of the CFAA, and on state-law claims for breach of contract and conversion. Dear moves to dismiss these claims under Rule 12(b)(6) for failure to state a claim on which relief can be granted.

II

In deciding Dear's Rule 12(b)(6) motion, the court evaluates the sufficiency of MBL's complaint by "accept[ing] 'all well-pleaded facts as true, viewing them in the light most favorable to the plaintiff.'" *In re Katrina Canal Breaches Litig.*, 495 F.3d 191, 205 (5th Cir. 2007) (quoting *Martin K. Eby Constr. Co. v. Dallas Area Rapid Transit*, 369 F.3d 464, 467 (5th Cir. 2004)). To survive the motion, MBL must plead enough facts "to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, ___ U.S. ___, 129 S.Ct. 1937, 1949 (2009). "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.*; see also *Twombly*, 550 U.S. at 555 ("Factual allegations must be enough to raise a right to relief above the speculative level[.]"). "[W]here the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has

alleged—but it has not ‘shown’—that the pleader is entitled to relief.” *Iqbal*, 129 S.Ct. at 1950 (alteration omitted) (quoting Rule 8(a)(2)).

III

The court turns initially to whether MBL has stated a plausible claim under the CFAA. Dear maintains, first, that he had authorization to access the MBL Gross Profit Report and that he did not exceed his authority by accessing or downloading it on February 28, 2010. He argues, second, that MBL has not sufficiently pleaded facts to show damages or loss in excess of \$5,000.

A

The Fifth Circuit has interpreted the CFAA to encompass limits placed on *the use* of information obtained by permitted access to a computer system and data available on that system. See *United States v. John*, 597 F.3d 263, 271 (5th Cir. 2010) (“The question before us is whether ‘authorized access’ or ‘authorization’ may encompass limits placed on *the use* of information obtained by permitted access to a computer system and data available on that system.”). In *John*, a criminal case, the panel addressed the defendant’s contention that the evidence was insufficient to convict her of violating the CFAA because “the statute [did] not prohibit unlawful use of material that she was authorized to access through authorized use of a computer.” *Id.* The defendant contended that the “statute only prohibits using authorized access

to obtain information that she is not entitled to obtain or alter information that she is not entitled to alter." *Id.* Rejecting the defendant's argument, the panel noted that, in *United States v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007), when analyzing whether a criminal defendant had accessed computers "without authorization," the Fifth Circuit had applied "intended-use analysis." *John*, 597 F.3d at 271. In *John* the defendant's use of the computer system to perpetrate fraud was not an intended use of that system. The defendant's use of the computer system to perpetrate a fraud was also contrary to the employer's policies. *Id.* at 272. In support of this latter conclusion, the *John* panel cited the First Circuit's decision in *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001). In that case the plaintiffs sued under CFAA for injunctive relief against former employees (now competitors) who had used knowledge obtained during their employment to mine their former employer's public website for pricing information. The former employees had entered into a broad confidentiality agreement protecting proprietary information. Based on this confidentiality agreement, the First Circuit held that their actions exceeded "authorized access," within the meaning of § 1030(a)(4). Although the *John* panel cautioned that it did not "necessarily agree that violating a confidentiality agreement under circumstances such as those in *EF Cultural Travel BV* would give rise to criminal culpability, [it did] agree with the First Circuit

that the concept of 'exceeds authorized access' may include exceeding the purposes for which access is 'authorized.'" *John*, 597 F.3d at 272. The panel concluded that "[a]ccess to a computer and data that can be obtained from that access may be exceeded if the purposes for which access has been given are exceeded." *Id.* The panel concluded that

the Government demonstrated at trial that [the defendant's employer's] official policy . . . prohibited misuse of the company's internal computer systems and confidential customer information. Despite being aware of these policies, [the defendant] accessed account information for individuals whose accounts she did not manage, removed this highly sensitive and confidential information from [the employer's] premises, and ultimately used this information to perpetrate fraud on [the employer] and its customers.

Id.

MBL has pleaded a plausible CFAA claim against Dear because it has alleged facts that allow the court to draw the reasonable inference that Dear accessed the MBL computer system and the Gross Profit Report and then used it, in violation of the restrictive covenant agreement without MBL's express consent, to compete directly with MBL in the restricted geographical area, to solicit MBL customers to purchase the same type of products sold by MBL, and to engage in activities that undermine MBL's business opportunities.

B

Dear's second argument also lacks force. MBL alleges that Dear's actions resulted in "damage or loss to MBL aggregating at least \$5,000 in value." Compl. ¶ 32. This allegation is augmented by factual assertions that meat products were sold to specific customers listed in MBL's Gross Profit Report. These averments make plausible MBL's theory that Dear obtained confidential business information while exceeding his authorized access, then used this customer data to deprive MBL of sales from regular customers, resulting in lost revenue that could amount to over \$5,000 over the course of one year.²

Accordingly, the court denies Dear's motion to dismiss MBL's claim under the CFAA.

IV

Dear also moves to dismiss MBL's breach of contract claim. This cause of action is based on two grounds—"use" of confidential information, in breach of § 1(a) of the covenant,³ and solicitation

²See 18 U.S.C. §§ 1030(c)(4)(A)(i)(I) and (g) (requiring loss aggregating at least \$5,000 in value "during any 1-year period" for a civil action to be maintained, and limiting damages to "economic damages").

³Section 1(a):

Employee shall not, without the prior written consent of the Employer, use, divulge, disclose or make accessible to any other person, firm, partnership, corporation or other entity any Confidential Information (as defined below) pertaining to the business of

of customers of MBL, in breach of § 1(b) of the covenant. Because MBL had pleaded a plausible claim based on a breach of § 1(a), the court in its discretion will not address the other grounds of Dear's motion or of MBL's breach of contract claim.

Dear maintains that he cannot have breached § 1(a) because MBL does not allege that he used or disclosed confidential information. The court disagrees. Although MBL does not assert that Dear disclosed to anyone else any part of the customer information he downloaded, MBL alleges that "Dear has utilized the contents of the MBL Gross Profit Reports and information contained therein to successfully solicit and sell meat products to several of the accounts listed on the MBL Gross Profit Reports." Compl. ¶ 24.

Dear next argues that Illinois law does not recognize

the Employer, except (i) while employed by the Employer, in the business of and for the benefit of the Employer, or (ii) when required to do so by a court of competent jurisdiction, or by any governmental agency having the lawful power to order such disclosure "Confidential Information" shall mean non-public information concerning the financial data, strategic business plans, product development (or other proprietary product data), trade secrets, customer names and lists, supplier and vendor names and lists, information made available to Employee while employed by Employer relating to customers, suppliers, and vendors, marketing plans, efforts, and techniques, and other non-public, proprietary and confidential information of the Employer.

Compl. Ex. A at 2.

information about MBL's customers as confidential. Under Illinois law, when evaluating the enforceability of a restrictive covenant on employment, a court must consider not only the reasonableness of the covenant but also whether the "plaintiff has proven the existence of a protectable business interest or property right[.]" *Image Supplies, Inc. v. Hilmert*, 390 N.E.2d 68, 70-71 (Ill. App. Ct. 1979). A restrictive covenant may be enforced "if the employee learned trade secrets or other confidential information while in plaintiff's employ and subsequently attempted to use it for his or her own benefit." *Springfield Rare Coin Galleries v. Mileham*, 620 N.E.2d 479, 485 (Ill. App. Ct. 1993). If, as a matter of law, the information Dear used cannot be deemed "confidential," then Dear cannot be found in violation of § 1(a).

The court will not deem MBL's customer listings to be confidential information based merely on the allegation in the complaint that they are. Although the court accepts the well-pleaded factual assertions of the complaint as true for the purposes of deciding Dear's Rule 12(b)(6) motion, it does not accept the complaint's legal conclusions as true. The restrictive covenant in question provides that "[t]his Agreement shall be construed, interpreted and governed in accordance with the laws of Illinois, without reference to rules relating to conflicts of law." Compl. Ex. A at 3. Therefore, to evaluate whether MBL has pleaded a plausible claim, i.e., whether MBL's customer listings qualify as

confidential information, the court turns to Illinois law for guidance.

In *Schulenburg v. Signatrol, Inc.*, 212 N.E.2d 865 (1965), the Illinois Supreme Court explained the following distinction for determining what the employer may restrict as confidential:

It is clear that an employee may take with him, at the termination of his employment, general skills and knowledge acquired during his tenure with the former employer. It is equally clear that the same employee may not take with him confidential particularized plans or processes developed by his employer and disclosed to him while the employer-employee relationship exists, which are unknown to others in the industry and which give the employer advantage over his competitors.

Id. at 869. Specifically, regarding customer information, Illinois courts have recognized restrictive covenants to cover a protectable business interest where "a trade secret or a near-permanent customer relationship exists which an employee learned of through his employment[.]" *Lincoln Towers Ins. Agency v. Farrell*, 425 N.E.2d 1034, 1036 (Ill. App. Ct. 1981).

The court will assume *arguendo* that MBL has not adequately pleaded that a near-permanent customer relationship exists. Even so, Dear is not entitled to dismissal of the component of MBL's breach of contract claim based on § 1(a) of the covenant if MBL has adequately pleaded facts that make the plausible showing that the Gross Profit Report qualifies as confidential information based on status as a trade secret or under the general guidelines in

Schulenburg.

The Illinois Supreme Court describes a trade secret as a "plan or process, tool, mechanism or compound known only to its owner and those of his employees to whom it is necessary to confide it." *Victor Chem. Works v. Iliff*, 132 N.E. 806, 811 (1921); accord *Schulenburg*, 212 N.E.2d at 868. The following factors are considered significant in determining whether something is a trade secret:

(1) the extent to which the information is known by others in the field; (2) the extent to which the information is known by the business' employees; (3) the extent to which the employer takes measures to guard the secrecy of the information; (4) the value of the information to the employer and his competitor; (5) the amount of effort or money spent in developing the information; and (6) the ease or difficulty in acquiring or duplicating the information.

Lincoln Towers, 425 N.E.2d at 1037 (citing *ILG Indus., Inc. v. Scott*, 273 N.E.2d 393, 396 (1971)). Furthermore, Illinois courts have held that a customer list or other customer information constitutes a trade secret where "the list has been developed by the employer over a number of years, the employer developed the list at great expense, and the information was kept under lock and key." *Id.* at 1038 (citations omitted). They have held that the same type of information is not a trade secret where

it has not been treated as confidential and secret by the employer, was generally available to other employees, the information was known to those in the field or could be easily duplicated . . . and where customers did business with more than one company or otherwise changed businesses frequently so that they were known to an employer's competition.

Id. (citations omitted).

If the complaint merely alleged that Dear took MBL's list of customers and used it for his personal benefit, then under the relevant factors it would not have adequately pleaded that the list qualifies as a trade secret or that Dear breached the contract on this basis. By using local directories or by canvassing the streets, competitors can easily duplicate a list of local restaurants, hotels, and other establishments that serve meat. But MBL has pleaded a claim based on a Gross Profit Report that contains more than names: it includes pricing information, costs and profit margins per customer, and observations developed over several years about customer product preferences. See Compl. ¶ 49. MBL alleges that this information had been developed over a number of years at great cost and that the information is password-protected with access granted only on a need-to-know basis. The well-pleaded facts show that MBL *treated* the information as confidential; the question becomes whether MBL has sufficiently pleaded that the information is in fact confidential. For example, in *Midwest Micro Media, Inc. v. Machotka*, 395 N.E.2d 188, 192 (Ill.

App. Ct. 1979), the court concluded that information that was "developed totally through [an employee's] own work efforts" could not constitute confidential information because such information was part of the employee's "general skills and knowledge acquired during his tenure with the former employer[.]" And in *Lincoln Towers* the court credited an expert witness' testimony that competitors could easily discover prices charged by others by speaking with their customers, even though a customer might lie. See *Lincoln Towers*, 425 N.E.2d at 1039.

The court holds that MBL has made a plausible claim that at least some of the contents of the Gross Profit Report—such as the information about profit margins or customer preferences—qualify as confidential information that is protectable under Illinois law as a trade secret. The MBL Gross Profit Report appears to contain more than Dear's accounts, see, e.g., Compl. Ex. B at 1-4 (indicating entries marked by different salesperson IDs), such that the customer information amounts to more than a mere summation of Dear's "knowledge acquired during his tenure." Moreover, even if Dear or another competitor of MBL could investigate customer prices independently (as in *Lincoln Towers*), without the Gross Profit Report he would still lack knowledge of MBL's profit margins and years of MBL's accumulated knowledge about customer preferences. If, as MBL alleges, such information was only obtained at great cost over years of observation, then permitting Dear to take this

information at no cost would instantly give a competitor what it took MBL years to develop. Given the well-pleaded facts, it is plausible that Dear not only used the names of the customers, but also used knowledge about customer preferences and profit margins to select which of MBL's customers to solicit for his own business. Therefore, MBL has pleaded a plausible claim for breach of contract of § 1(a) of the covenant by alleging that, after resigning from MBL, Dear used for his own purposes one of MBL's trade secrets.

Dear's motion to dismiss MBL's breach of contract claim is denied.⁴

V

Dear also moves to dismiss MBL's conversion claim on the ground that Texas law does not recognize a cause of action for the conversion of intellectual property, such as trade secrets. The court agrees.

"Texas law has never recognized a cause of action for conversion of intangible property except in cases where an underlying intangible right has been merged into a document and that document has been converted." *Express One Int'l, Inc. v.*

⁴MBL also raises for the first time in its response brief the contention that Dear breached his fiduciary duty to MBL by soliciting customers for himself during his employment. "[I]t is axiomatic that the Complaint cannot be amended by the briefs in opposition to a motion to dismiss." *In re Sec. Litig. BMC Software, Inc.*, 183 F.Supp.2d 860, 915 (S.D. Tex. 2001) (quoting *In re Baker Hughes Sec. Litig.*, 136 F.Supp.2d 630, 646 (S.D. Tex. 2001)). The court therefore declines to consider this argument.

Steinbeck, 53 S.W.3d 895, 901 (Tex. App. 2001, no pet.); see *Procom Cable TV Serv., Inc. v. Paragon Commc'n*, 1994 WL 406013, at *3 (Tex. App. Aug. 4, 1994, no writ) (not designated for publication) ("Only tangible personal property is subject to a suit for conversion.") (citing, *inter alia*, *U.S. Sporting Prods., Inc. v. Johnny Stewart Game Calls, Inc.*, 865 S.W.2d 214, 222 (Tex. App. 1993, writ denied)); cf. *Quantlab Techs. Ltd. (BVI) v. Godlevsky*, 719 F.Supp.2d 766, 779 (S.D. Tex. 2010) (noting two ambiguous cases but declining to depart from the interpretation of Texas law "shared by the majority of Texas courts and the Fifth Circuit," and holding that "conversion applies only to physical property under Texas law"). MBL's lawsuit is based on intangible property: the confidential information that Dear allegedly obtained when he accessed MBL's computer system. MBL has not pleaded a plausible conversion claim, and the court grants Dear's Rule 12(b)(6) motion in this respect.

VI

Although the court is in part granting the motion to dismiss, it will permit MBL to replead. Courts often grant a plaintiff one opportunity to replead, unless it appears that the plaintiff cannot cure the initial deficiencies in the pleading. See *In re Am. Airlines, Inc., Privacy Litig.*, 370 F.Supp.2d 552, 567-68 (N.D. Tex. 2005) (Fitzwater, J.) ("[D]istrict courts often afford plaintiffs at least one opportunity to cure pleading deficiencies


before dismissing a case, unless it is clear that the defects are incurable or the plaintiffs advise the court that they are unwilling or unable to amend in a manner that will avoid dismissal." (internal quotation marks and citation omitted)). Because there is no indication that MBL cannot, or is unwilling to, cure the defects that the court has identified, the court grants MBL 30 days from the date this memorandum opinion and order is filed to file an amended complaint.

* * *

For the reasons explained, the court grants in part and denies in part Dear's motion to dismiss. MBL may file an amended complaint within 30 days of the date this memorandum opinion and order is filed.

SO ORDERED.

April 20, 2011.



SIDNEY A. FITZWATER
CHIEF JUDGE